RFC-0009 Significant Change Notification Technical Assistance

Thursday, May 15th, 2025

Background

The FedRAMP Authorization Act (44 USC § 3609 (a) (3)) directs the Administrator of the General Services Administration to *"develop and publish templates, best practices, technical assistance, and other materials to support the authorization of cloud computing products and services and increase the speed, effectiveness, and transparency of the authorization process, consistent with standards and guidelines established by the Director of the National Institute of Standards and Technology and relevant statutes."* This responsibility is delegated to the FedRAMP Director.

OMB Memorandum M-24-15 on Modernizing FedRAMP section 2 states that *"FedRAMP should not incentivize or require commercial cloud providers to create separate, dedicated offerings for Federal use, whether through its application of Federal security frameworks or other program operations. The Federal Government benefits from the investment, security maintenance, and rapid feature development that commercial cloud providers give to their core products to succeed in the marketplace."*

The FedRAMP Significant Change Notification Standard [DRAFT] states *"All parties SHOULD follow FedRAMP's best practices and technical assistance on significant change assessment and notification where applicable."*

Introduction

This document, Significant Change Notification Technical Assistance, is intended to support cloud service providers and third-party assessment organizations in adopting the Significant Change Notification Standard.

Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

The Significant Change Notification Standard is designed for reasonable people to have reasonable discussions about changes that cloud services plan to make as they apply directly to their own specific cloud service. Cloud service providers are expected to employ competent technical security staff and involve them in product and engineering decisions to properly assess changes before, during, and after such changes.

Decisions should be reasonable, defensible, and documented. The Significant Change Notification Standard should be used directly. This Technical Assistance provides additional background but is not intended to replace the Significant Change Notification Standard.

This Technical Assistance will be continuously expanded as the Significant Change Notification Standard is formalized, based on concerns raised during public comment and ongoing support and operations of FedRAMP. The RFC process may not apply to future versions.

Determining Significant Changes

The cloud service provider is solely responsible for determining when the FedRAMP Significant Change Notification Standard should be applied and for determining if a significant change is an adaptive change, transformative change, or impact categorization change. Cloud service providers do not need to consult with third-party assessment organizations if the provider determines the change is adaptive.

The simplest way to determine the type of significant change is to determine if it's a routine recurring change then work down from the highest impact change type:

1. If a change is significant, is it a routine recurring activity?
2. If it is not, is it an impact categorization change?
3. If it is not, is it a transformative change?
4. If it is not, then it is an adaptive change.

In general, the vast majority of significant changes made by cloud service providers where the Significant Change Notification Standard applies will be adaptive changes.

Is it a routine recurring activity?

Activities that are part of ongoing operations or vulnerability mitigation and remediation are NOT considered significant changes.

These types of activities are performed regularly and routinely by cloud service providers to address flaws or vulnerabilities, address incidents, and generally perform the typical maintenance expected during day-to-day operations.

These changes leverage mature processes and capabilities to identify, mitigate, and remediate risks as part of the change. Change management and incident response procedures of the cloud service provider are assessed during the Authority to Operate decision process by the agency customer(s).

Ongoing Operations: Changes performed regularly and routinely without significant planning or oversight.

Key Tests:

- Routine “care and feeding” by staff during normal duties
- Careful planning and/or project management NOT required
- No major impact to service availability

Examples:

- Provisioning or deprovisioning capacity to support service elasticity
- Changing or tuning performance configurations for instances or services
- Updating and maintaining operational handling of information flows and protection across physical and logical networks (e.g., updating firewall rules)
- Generating or refreshing API or access tokens

Vulnerability mitigation and remediation: Updates and patching performed on a routine basis to improve the security posture over time.

Key Tests:

- Minor, incremental patching or updates
- Significant refactoring or migration process NOT required
- No breaking changes

Examples:

- Updating security service or endpoint signatures
- Routine patching of devices, operating systems, software or libraries
- Updating and deploying code that applies normal fixes and improvements as part of a regular development cycle
- Vulnerability remediation activity that simply replaces a known-bad component(s) with a better version of the exact same thing, running in the exact same way with no changes to processes

Significant Changes that Require Authorization Updates

Is it an impact categorization change?

Impact categorization changes are perhaps the simplest to identify in the current framework - if the intent of the change is to increase or decrease the FIPS 199 security categorization (impact level) *of the entire system* (such as from Low to Moderate or from High to Moderate) then it is an impact categorization change.

Impact categorization changes require review and approval of either FedRAMP or a sponsoring agency and will lead to a re-authorization of the service at the new impact level.

Significant Changes that Require Notification

Is it a transformative change?

Change that impacts major components or functionality and profoundly affects a cloud service offering is considered a transformative change.

Major components or functionality: Components or capabilities critical and foundational to cloud service operations and risk profile.

> *NOTE: Major components or functionality is determined for the specific offering and a change that is transformative for one service may not be for another service.*

Key Tests:

- Alters the service's risk profile or require new or significantly different actions to address customer responsibilities
- Requires significant new design, development and testing with discrete associated project planning, budget, marketing, etc.
- Requires extensive updates to security assessments, documentation, and how a large number of security requirements are met and validated

Examples:

- The addition, removal, or replacement of a critical third party service that handles a significant portion of information (e.g., IaaS change)
- Increasing the security categorization of a service within the offering that actively handles federal information (does NOT include impact change of entire offering - see impact categorization change)
- Replacement of underlying management planes or paradigm shift in workload orchestration (e.g., bare-metal servers or virtual machines to containers, migration to kubernetes)
- Datacenter migration where large amounts of federal information is moved across boundaries different from normal day-to-day operations

Is it an adaptive change?

Change that is not routine, does not change the impact categorization of the service offering and does not greatly impact major components or functionality (transformative change) is considered an adaptive change.

Service adjustments: Iterative adjustments to existing components or functionality which is not routine, but not a complete redesign or overhaul.

Key Tests:

- Requires few changes to security plans or procedures
- Requires some careful planning and project management to implement, but doesn't rise to the level of planning required for transformative changes
- Requires verification of existing functionality and secure configuration after implementation

Examples:

- Updates to operating systems, containers, virtual machines, software or libraries with known breaking changes, complex steps, or service disruption
- Deploying larger than normal incremental feature improvements in code or libraries that are the work of multiple weeks of development efforts but aren't considered a major new service
- Changing cryptographic modules where the new module meets the same standards and characteristics of the former
- Replacing a like-for-like component where some security plan or procedure adjustments are required (e.g., scanning tool or managed database swap)